GATE 15
ANALYSIS • RESILIENCE • OPERATIONS

Job Opening Announcement

OT Cyber Threat Analyst

Role – OT Cyber Threat Analyst (3+ years of cybersecurity experience, including 2+ years supporting OT/ICS environments).

Location – Remote, with occasional travel to client sites.

General Description – Gate 15 is seeking an OT Cyber Threat Analyst to help protect the systems that run critical infrastructure, including energy, water and wastewater, manufacturing, transportation, and building automation. You will track threats ranging from ransomware that spills over from IT into OT networks, to nation-state actors pre-positioning in utilities, to hacktivists tampering with internet-exposed controllers.

This is a two-part role. Most of your time will go to producing and sharing OT threat intelligence. You will also serve as an OT subject matter expert for our clients, supporting security assessments and working directly with engineers and plant operators to turn findings into practical recommendations that reflect how industrial processes actually run.

What You Will Do

Threat Intelligence

- Monitor open-source, commercial, vendor, and partner reporting for emerging threats, active campaigns against industrial sectors, and newly disclosed or exploited ICS vulnerabilities.
- Track ransomware groups, cybercriminals, hacktivists, and nation-state actors, and assess their intent, capability, and likely targeting of critical infrastructure.
- Share indicators, adversary TTPs, and ICS vulnerability advisories with DHS/CISA, the FBI, sector ISACs, and owner/operator partners, and support partners during significant cyber incidents.
- Respond to requests for information and produce threat bulletins, threat actor profiles, vulnerability advisories, and incident summaries.

OT Advisory & Assessments

- Support client OT risk assessments by reviewing network architectures, asset inventories, remote access pathways, and monitoring data.
- Assess what threats and vulnerabilities mean for safety, reliability, and physical operations, including how an incident could cascade across interdependent sectors.
- Develop prioritized, operationally feasible recommendations (e.g., segmentation, compensating controls, monitoring improvements, and patching aligned to maintenance windows) that do not compromise safety or availability.

Products & Communication

- Brief engineers, plant operators, and executives, translating technical findings into clear, actionable guidance.
- Create data visualizations, SOPs, and product templates that support client reporting and information-sharing workflows.

Minimum Qualifications

- Must be a citizen of the United States.
- Must have 3+ years of experience in cyber threat intelligence, security operations, incident response, OT/ICS security, or a related role, including at least 2 years working in or directly supporting OT/ICS environments (e.g., at an asset owner, ISAC, OT security vendor, integrator, or OT-focused consultancy).
- Hands-on understanding of how industrial control systems work, including PLCs, HMIs, SCADA and DCS architectures, the Purdue Model, and common industrial protocols such as Modbus, DNP3, and OPC UA.
- Understanding of how security actions such as patching, active scanning, network changes, or isolating a system can affect safety and operational availability.
- Working knowledge of the OT threat landscape (common intrusion paths, notable ICS malware and campaigns, and the actors behind them) and frameworks such as MITRE ATT&CK for ICS.
- Strong analytic writing and briefing skills: you can pull what matters out of technical reporting and explain it clearly to both technical and non-technical audiences.
- Availability for after-hours, holiday, and weekend on-call support during heightened threat conditions and significant incidents.
- A degree in cybersecurity, computer science, information systems, electrical or controls engineering, intelligence studies, or a related field, or equivalent military, trade, or hands-on industrial/OT experience.

Preferred Qualifications

- Experience at an ISAC, fusion center, SOC/CSIRT, or government cyber intelligence role, or at a utility or other industrial asset owner.
- An industrial background such as controls engineering, plant operations, or instrumentation, especially in energy, water and wastewater, building automation, oil and gas, or transportation.
- Experience conducting or supporting OT security assessments using ISA/IEC 62443, NIST SP 800-82, NERC CIP, or CISA CSET.
- Experience with OT monitoring and threat intelligence tools such as Dragos, Claroty, Nozomi Networks, Microsoft Defender for IoT, MISP, ThreatConnect, Splunk, Shodan, or Censys.
- Familiarity with the Diamond Model, ICS Cyber Kill Chain, Traffic Light Protocol (TLP), STIX/TAXII, and the CISA Known Exploited Vulnerabilities catalog.

- Basic scripting or query skills (e.g., Python, SQL, or KQL) and packet analysis of industrial protocol traffic with tools such as Wireshark.
- Certifications such as GICSP, GRID, GCTI, ISA/IEC 62443, CompTIA Security+, or CySA+.
- Intelligence analyst training from the FEMA-approved course list for the Homeland Security Grant Program.

Next Steps – If your application looks like a match, someone from our team may reach out to schedule a phone screening. During this conversation, we will determine if the position aligns with your experience and skills. If things go well, from there you will meet with members from the project team, including the hiring manager and teammates, and possibly be asked to prepare a presentation, complete an OT scenario exercise (for example, analyzing a hypothetical incident involving an industrial control system and identifying the risks, potential operational consequences, and recommended actions), submit a writing sample, or something else to showcase your practical knowledge. If we find you are a match, you will get a call offering you the role. While we wish we could hire every great candidate who comes our way, we cannot. If you are not selected, we will be sure to connect with you and let you know so you can move on with your search. We will also keep your resume for future needs.

About Gate 15 – Gate 15 is a Service-Disabled Veteran-Owned Small Business (SDVOSB) focused on helping homeland security partners address their most pressing and complex challenges and opportunities. The company provides risk management consulting services to the homeland and national security enterprise across three areas: analysis, resilience, and operations. Learn more at www.gate15.global.

We value a diverse, inclusive workforce and provide equal employment opportunities for all applicants and employees. It is the policy of Gate 15 to comply with all federal and state laws concerning the employment of persons with disabilities, and to act in accordance with regulations and guidance issued by the Equal Employment Opportunity Commission (EEOC) and state agencies. All qualified applicants for employment will be considered without regard to an individual's race, color, sex, gender identity, gender expression, religion, age, national origin or ancestry, citizenship, physical or mental disability, medical condition, family care status, marital status, domestic partner status, sexual orientation, genetic information, military or veteran status, or any other basis protected by federal, state, or local laws. Gate 15 is a drug-free workplace.

Interested candidates should submit their resume to HR@gate15.global.

No phone calls will be accepted.

We look forward to reviewing your application soon!